CLAIMS

We claim:

1. A method of connecting an end user associated with a first organization to an application hosted by a second organization while providing double blind authentication wherein the identity of the end user is kept from the second organization and the identity of the second organization is hidden from the end user, the method comprising the steps of:

exchanging digital certificates between the first organization and the second organization;

sending an authenticated and encrypted first message using the digital certificate from the first organization to the second organization, wherein the first message requests a virtual user ID for use by the end user;

validating the digital certificate and decrypting the first message sent by the first organization at the second organization;

responding to the first message by sending an authenticated and encrypted response message comprising an authorized virtual user ID from the second organization to the first organization;

authenticating the end user at the first organization;

mapping an end user's user ID to the virtual user ID;

sending an authenticated and encrypted second message from the first organization to the second organization, the second message including a session initialization request; and

replying to the second message at the second organization with an authenticated and encrypted reply message comprising a session ID.

2. The method of claim 1, wherein the step of sending the authenticated and encrypted first message further comprises:

sending a subsequent authenticated and encrypted message from the first organization to the second organization requesting to modify the authorized virtual user ID for a specific end user; and

acknowledging the subsequent message by sending a different authenticated and encrypted message from the second organization to the first organization including an appropriate virtual user ID for the specific end user.

3. The method of claim 1, further comprising the step of monitoring the session ID to ensure that an end user's session does not become stale.

4. The method of claim 1, wherein the step of authenticating the end user at the first organization is performed after the end user logs on to a web server associated with the first organization.

5. The method of claim 1, wherein the steps of sending the authenticated and encrypted first message, sending the authenticated and encrypted second message, responding to the first message by sending the authenticated and encrypted response message, and replying to the second message at the second organization with the authenticated and encrypted reply message, are performed using Public Key Infrastructure technology.

6. The method of claim 1, wherein the step of exchanging digital certificates is performed via a manual process.

7. The method of claim 6, wherein the manual process is selected from one of U.S. Mail, Courier Mail, or messenger.

8. The method of claim 1, wherein the step of replying to the second message includes passing the session ID as a cookie.

9. The method of claim 1, wherein the step of replying to the second message includes authorizing the end user for use of at least one application associated with the second organization.

10. The method of claim 1, wherein the existence of the second organization remains hidden from the end user.

11. The method of claim 1, wherein the steps of sending the first and the second messages each further comprise the step of sending the first message or the second message over an electronic network.

12. The method of claim 11, wherein the electronic network is one of the internet, a telephone line, and a dedicated line.

13. The method of claim 1, wherein the method of connecting the end user

associated with the first organization to the application hosted by the second organization is performed by connecting the end user to the application via an electronic network.

14. The method of claim 1, wherein the first organization and the second organization are financial institutions.

15. A system for connecting an end user associated with a first organization having a first processor to an application hosted by a second organization having a second processor while providing double blind authentication wherein the identity of the end user is kept from the second organization and wherein the identity of the second organization is hidden from the end user, and wherein an electronic network connects the first organization to the second organization, the system comprising:

a first memory and a second memory;

a first software routine stored in the first memory and adapted to be executed on the first processor to execute the steps of;

1) sending an authenticated and encrypted first message using a first digital certificate from the first organization to the second organization requesting an authorized virtual user ID for use by the end user;

2) authenticating the end user;

3) mapping an end user's user ID to an authorized virtual user ID; and

4) sending an authenticated and encrypted second message from the first organization to the second organization, the second message including a session initialization request; and

a second software routine stored in the second memory and adapted to be executed on the second processor to execute the steps of;

1) validating the first digital certificate;

2) decrypting the first message sent by the first software routine;

3) responding to the first message by sending an authenticated and encrypted response message comprising the authorized virtual user ID; and

4) replying to the second message with an authenticated and encrypted reply message using a second digital certificate, wherein the reply message includes a session ID.

16. The system of claim 15, wherein the first software routine is further adapted to perform the step of sending a subsequent authenticated and encrypted message from the first organization to the second organization requesting to modify the authorized virtual user ID for a specific end user; and

wherein the second software routine is further adapted to perform the step of acknowledging the subsequent message by sending a different authenticated and encrypted message from the second organization to the first organization including an appropriate virtual user ID for the specific end user.

17. The system of claim 15, wherein the second software routine stored in the second memory is adapted to perform the step of monitoring the session ID to ensure that an end user's session does not become stale.

18. The system of claim 15, wherein the first software routine stored in the first

memory is adapted to perform the step of authenticating the end user after the end user logs on to a web server located at the first organization.

19. The system of claim 15, wherein the first software routine is adapted to authenticate and encrypt the first message and the second message and the second software routine is adapted to authenticate and encrypt the response message and the reply message using Public Key Infrastructure technology.

20. The system of claim 15, wherein the first software routine is adapted to receive and store the first digital certificate and the second software routine is adapted to receive and store the second digital certificate.

21. The system of claim 15, wherein the second software routine stored in the second memory is adapted to perform the step of replying to the second message with an authenticated and encrypted reply message including a session ID by passing the session ID as a cookie.

22. The system of claim 15, wherein the session ID includes an authorization for at least one application for use by the end user.